APPENDIX C

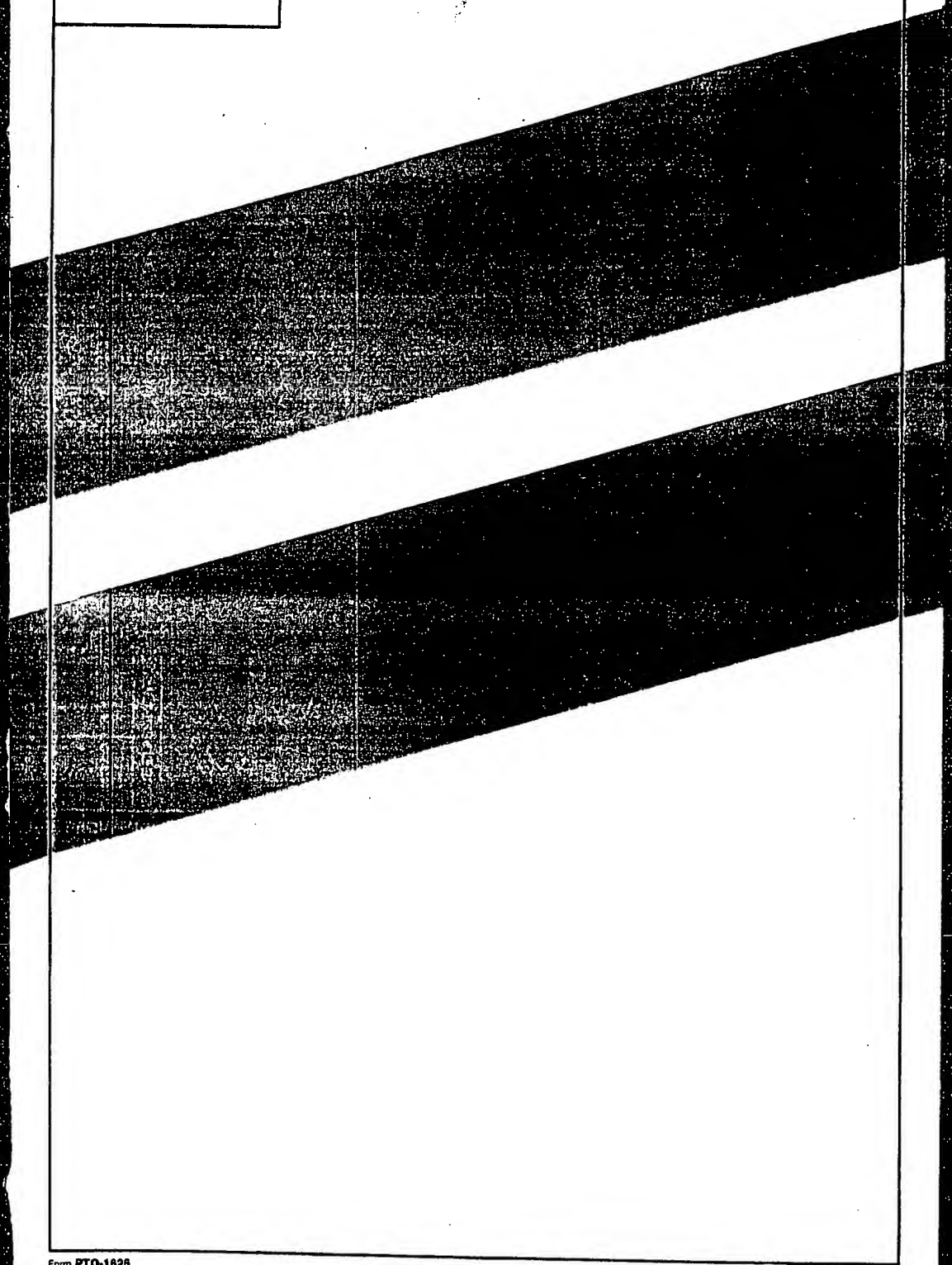
(Copy of U.S. Patent No. 60/206,186, filed on May 22, 2000)

(Obtained from the Group Art Unit at the United States Patent and Trademark Office)

05/22/00

ISSUE CLASSIFICATION	Class	Subclass

PROVISIONAL APPLICATION NUMBER



Form PTO-1625
(Rev. 6/99)

(FACE)

Bib Data Sheet

UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

SERIAL NUMBER	FILING DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
60/206,186	05/22/2000 RULE –	–	–	040020-270

APPLICANTS

Ina Widegren, Stockholm, SWEDEN;
Gabor Fodor, Hasselby, SWEDEN;
Brian Williams, Melbourne, Victoria, AUSTRALIA;
Johnson Oyama, Residence Not Provided;

** CONTINUING DATA **********

** FOREIGN APPLICATIONS **********

IF REQUIRED, FOREIGN FILING LICENSE GRANTED
** 06/08/2000 –

Foreign Priority claimed	☐ yes ☐ no	STATE OR COUNTRY	SHEETS DRAWING	TOTAL CLAIMS	INDEPENDENT CLAIMS
35 USC 119 (a-d) conditions met	☐ yes ☐ no ☐ Met after Allowance	SWEDEN	–	–	–
Verified and Acknowledged	Examiner's Signature Initials				

ADDRESS

–

Ronald L Grudziecki
Burns doane Swecker & Mathis L L P
Post Office Box 1404
Alexandria ,VA 22313-1404

TITLE

All ip policy architecture

FILING FEE RECEIVED	FEES: Authority has been given in Paper	☐ All Fees
150	No. _____ to charge/credit DEPOSIT ACCOUNT	☐ 1.16 Fees (Filing)
	No. _____ for following:	☐ 1.17 Fees (Processing Ext. of time)
		☐ 1.18 Fees (Issue)
		☐ Other _____
		☐ Credit

PATENT APPLICATION

60206186

INITIALS

CONTENTS

Date Received or Mailed

1.
2.
3.
4.
5.
6.
7.
8.
9.
10.
11.
12.
13.
14.
15.
16.
17.
18.
19.
20.
21.
22.
23.
24.
25.
26.
27.
28.
29.
30.
31.
32.

(LEFT OUTSIDE)

05-23-00 A/PROV

PTO/SB/16 (11-95)
Approved for use through 01/31/98. OMB 0651-0037
Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

05/22/00 JC531 U.S. PTO

PROVISIONAL APPLICATION FOR PATENT COVER SHEET

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53(c).

05/22/00 JC531 U.S. PTO 09/576186

Docket Number	040020-270	Type a plus sign (+) inside this box	+

INVENTOR(s)/APPLICANT(s)

LAST NAME	FIRST NAME	MIDDLE INITIAL	RESIDENCE (CITY AND EITHER STATE OR FOREIGN COUNTRY)
Widegren	Ina		Stockholm, SWEDEN
Fodor	Gabor		Hässelby, SWEDEN

TITLE OF THE INVENTION (280 characters max)

All IP Policy Architecture

CORRESPONDENCE ADDRESS

Ronald L. Grudziecki
BURNS, DOANE, SWECKER & MATHIS, L.L.P.
Post Office Box 1404
Alexandria

STATE	Virginia	ZIP CODE	22313-1404	COUNTRY	United States of America

ENCLOSED APPLICATION PARTS *(check all that apply)*

- [X] Specification — *Number of Pages* 19
- [ ] Drawing(s) — *Number of Sheets* ____
- [ ] Small Entity Statement
- [ ] Other (specify)

METHOD OF PAYMENT OF FILING FEES FOR THIS PROVISIONAL APPLICATION FOR PATENT *(check one)*

[ ] A check or money order is enclosed to cover the Provisional filing fees	PROVISIONAL FILING FEE AMOUNT(S)	$150.00
[X] The Commissioner is hereby authorized to charge any deficiency in filing fees or credit any overpayment to Deposit Account Number 02-4800. This paper is submitted in triplicate.		

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

- [X] No.
- [ ] Yes, the name of the U.S. Government agency and the Government contract number are:

Respectfully submitted,

SIGNATURE Michael G. Savage Date May 22, 2000

TYPED or PRINTED NAME Michael G. Savage Registration No. 32,596 *(if appropriate)*

[X] Additional inventors are being named on separately numbered sheets attached hereto.

21839

LAST NAME	FIRST NAME	MIDDLE INITIAL	RESIDENCE (CITY AND EITHER STATE OR FOREIGN COUNTRY)
Williams	Brian		Melbourne, Victoria, AUSTRALIA
Oyama	Johnson		

Invention Disclosure

1 TECHNICAL INFORMATION

1.1 Name of invention

All IP policy architecture

1.2 Inventor(s)

Name : Ina Widegren
Department : ERA Z/T
Employee no. : 331478
Phone no. : +46 8 757 18 23
e-mail/memo : ina.widegren@era.ericsson.se

Name : Gabor Fodor
Department : ERA T/N
Employee no. :
Phone no. : +46 8 4043084
e-mail/memo : gabor.fodor@era.ericsson.se

Name : Brian Williams
Department : EPA/D/FD
Employee no. :
Phone no. : +61 3 9301 4675
e-mail/memo : brian.williams@ericsson.com.au

Name : Johnson Oyama
Department : NRJ/RT/XT
Employee no. :
Phone no. : + 81-3-5216-9056
e-mail/memo : Johnson.Oyama@nrj.ericsson.se

1.3 Background

1.3.1 Abbreviations

3G 3rd Generation

BS	Bearer Service
CC	Call Control
CN	Core Network
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communication
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISDN	Integrated Services Digital Network
IPPC	IP Policy Control
MO	Mobile Originating Call
MT	Mobile Terminal
MTC	Mobile Terminated Call
NS	Network Service
PDP	Packet Data Protocol
PDU	Protocol Data Unit
PS	Packet Switched
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RAB	Radio Access Bearer
RAN	Radio Access Network
RSVP	Resource Reservation Protocol
RT	Real Time
RTP	Real Time Transport Protocol
SAP	Service Access Point
SDU	Service Data Unit
SGSN	Serving GPRS Support Node

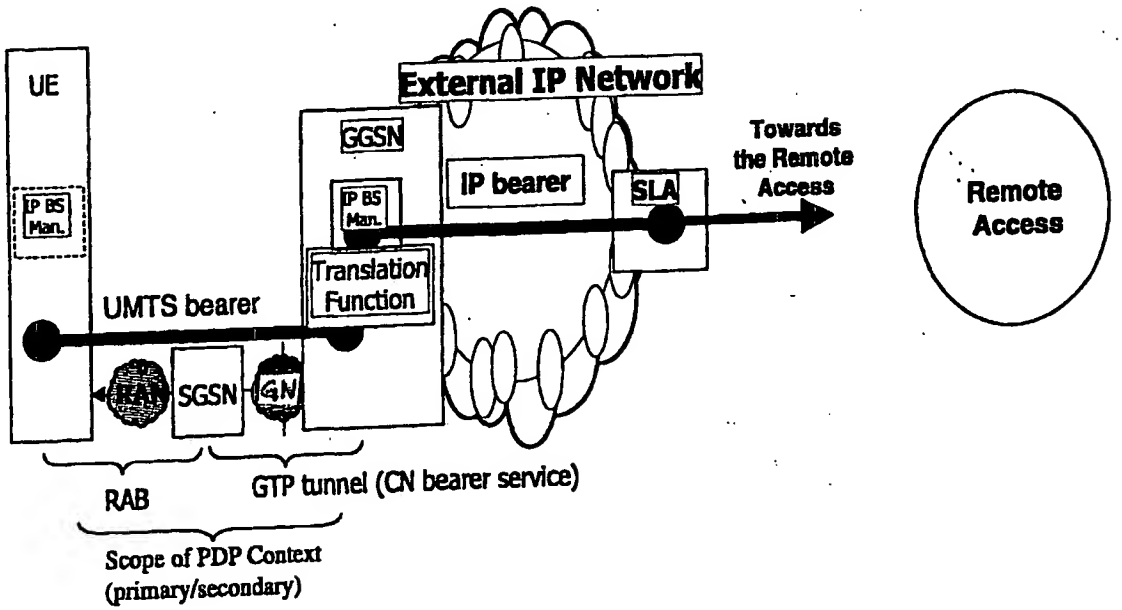
SLA	Service Level Agreement
UDP	User Datagram Protocol
TE	Terminal Equipment
TSPEC	Traffic Specification
UE	User Equipment
UMTS	Universal Mobile Telecommunication System
UTRA	UMTS Terrestrial Radio Access
UTRAN	UMTS Terrestrial Radio Access Network

1.3.2 Definitions

External Applications: Applications on an external Host.

User Equipment is a device allowing a user access to network services. For the purpose of 3GPP specifications the interface between the UE and the network is the radio interface. A User Equipment can be subdivided into a number of domains, the domains being separated by reference points. Currently defined domains are the USIM and ME Domains. The ME Domain can further be subdivided into several components showing the connectivity between multiple functional groups. These groups can be implemented in one or more hardware devices. An example of such a connectivity is the TE – MT interface.

The **Radio Access Network** domain consists of the physical entities, which manage the resources of the radio access network, and provides the user with a mechanism to access the core network. The Access Network Domain comprises roughly the functions specific to the access technology.


UE
IP BS Man.
External IP Network
GGSN
IP BS Man.
IP bearer
SLA
Towards the Remote Access
Remote Access
Translation Function
UMTS bearer
RAN
SGSN
GN
RAB
GTP tunnel (CN bearer service)
Scope of PDP Context (primary/secondary)

Title: IP Policy Architecture

1. Introduction

This contribution proposes an IP Policy Architecture applicable to UMTS.

2. Discussion

During the S2 R00 Drafting Meeting on QoS issues which took place in Stockholm on May 9-11, 2000, the following requirement was identified following the discussion of AT&T's contribution entitled "Integration of SIP Signalling and Resource Management in 3GPP" (S2-000723):

- the need for enabling mechanisms to transfer local policy decisions resulting from events in the application level (e.g., local SIP proxy) down to the IP bearer level (GGSN).

The requirement suggests the need for a suitable IP policy architecture which can interwork with the application layer, formulate local policy decisions, and enforce policy in the IP bearer level at the GGSN.

Recent developments in IETF surrounding IP policy framework and protocols reflect industry thrust in providing services with appropriate quality of service to users who are willing to pay for better than best effort services. Some relevant IETF RFC's on the subject matter include [RFC2573] "A Framework for Policy-based Admission Control", [RFC2748] "The COPS Protocol", [RFC2749] "COPS usage for RSVP", etc. Several Internet drafts are also being proposed which suggests possible extensions to the framework.

It is envisaged that the IP policy framework employed in UMTS would conform to IETF standards to leverage the expertise and developments in the mainstream IP community.

On the other hand, there already exist working UMTS policy mechanisms within the UMTS specifications like the TS23.107. As R00 is a smooth evolution from

R99 wherever possible, the UMTS policy mechanisms should continue to be used for control of the UMTS bearers.

It is important to allow separate evolution for UMTS policy mechanisms and IP policy framework, since the UMTS bearer services and IP bearer services have distinct QoS management roles along pertinent segments in the end-to-end path. This means that backward, as well as future compatibility for the respective functionalities should be ensured. It is thus envisaged that interaction between the two would occur only at well defined points to minimize interdependencies.

The IP BS Manager within the GGSN has been identified as being a policy enforcement point during the QoS drafting meeting in Stockholm (endorsed S2-000732). Also, the translation/mapping function within the GGSN must provide the interworking between the mechanisms and parameters used within the UMTS and the external IP bearer service (23.821 Section 9.2). Thus, the interaction between UMTS and IP policy mechanisms should effectively occur in the GGSN.

3. Proposal

New text on UMTS and IP QoS Policy Requirements is proposed. A new element "IP Policy Control" is also introduced in the R00 QoS model.

The following additions/modifications are proposed for Chapter 9 of TR23.821 Architecture Principles for Release 2000.

As Figure 9-1 of TR23.821 (a modification of Figure 2 in TS23.107) is of informational nature, additions to the figure, i.e., IP Policy Control element and related protocol interfaces, are attempted to help solve the QoS policy related concerns that have been identified so far. After a better understanding of requirements and subsequent agreement on appropriate solution within the QoS drafting group, it is to be determined what and how aspects of the proposal can be included in the normative portion of the R00 standard.

Note: The proposed changes are shown against TR23.821 V0.2.0 incorporating the already approved (endorsed by the QoS drafting meeting in Stockholm) texts in Tdoc. S2-000732 (IP BS Manager Capabilities) and Tdoc. S2-000735 (QoS Control of the IP Bearer Service).

9 QoS

[Note: The following sections are intended to be included in TS23.107 (proposed chapter, if any):

- 9.1.1 (new Chapter 4.4)
- 9.1.2 (new Chapter 4.5)
- 9.2 (Chapter 6.2)

9.1 Requirements

9.1.1 End-to-End QoS Negotiation Requirements

(no change)

9.1.2 QoS Policy Requirements

- The existing UMTS policy mechanisms shall continue to be used for control of the UMTS bearers. It is recognized that there already exists UMTS policy mechanisms within the existing UMTS specifications (in TS23.107).
- The IP policy framework employed in UMTS shall, as far as possible, conform to IETF "Internet Standards". The IETF policy framework shall be used for policy decision, authorization, and control of the IP level functionality, at both user and network level. This ensures conformance to mainstream IP developments.
- There shall be separation between the usage and roles of the UMTS policy mechanisms and the IP policy framework. This is to facilitate separate evolution of these functions. Interaction between UMTS bearer services and IP bearer services shall only occur at well defined points, thus ensuring the separation of the two policy architectures.

9.2 QoS End-to-End Functional Architecture

To provide QoS end-to-end, it is necessary to manage the QoS within each domain. An IP BS Manager is used to control the external IP bearer service. Due to the different techniques used within the IP network, this communicates to the UMTS BS manager through the Translation function.

To enable coordination between events in the application layer and resource management in the IP bearer layer, an element called IP Policy Control is used as a logical policy decision element that is local to the network providing resources for the bearer path, with protocol interfaces to local application servers/proxies, as well as to the GGSN where policy decisions are enforced.

The IP policy structure bases policy decisions only on information obtained from nodes / elements within the network which owns the resources for the bearer path, i.e., the local network.

In addition, it is possible to implement a policy decision element internal to the IP BS Manager in the GGSN. The IP policy architecture does not mandate the policy decision point to be external to the GGSN.

Whenever resources not owned or controlled by the UMTS network are required to provide QoS, it is necessary to interwork with an external resource manager that controls those resources.

IP BS Manager

The IP BS Manager uses standard IP mechanisms to manage the IP bearer service. These mechanisms may be different from mechanisms used within the UMTS, and may have different parameters controlling the service. The translation/mapping function provides the interworking between the mechanisms and parameters used within the UMTS and the external IP bearer service, and interacts with the IP BS Manager.

If an IP BS Manager exists both in the UE and the Gateway node, it is possible that these IP BS Managers communicate directly with each other by using relevant signalling protocols.

The required options in the table define the minimum functionality that shall be supported by the equipment in order to allow multiple network operators to provide interworking between their networks for end-to-end QoS. Use of the optional functions listed below, other mechanisms which are not listed (eg over-provisioning), or combinations of these mechanisms are not precluded from use between operators.

The IP BS Managers in the UE and GGSN provide the following set of capabilities for the IP bearer level:

Capability	UE	GGSN
DISSERVE EDGE FUNCTION	Optional	Required
RSVP/INTSERVE	Optional	Optional
IP POLICY ENFORCEMENT POINT	Optional	Required (°)

Provision of the IP BS Manager is optional in the UE, and required in the GGSN.

(°) Although the capability of IP policy enforcement is required within the GGSN, the control of IP policy through the GGSN is a network operator choice. Where the APN is not located at the GGSN, the location of policy enforcement point is for further investigation.

IP Policy Control

The IP Policy Control is a logical local policy decision element which uses standard IP mechanisms to implement policy in the IP bearer layer. These mechanisms may be conformant to, for example, the framework defined in IETF [RFC2753] "A Framework for Policy-based Admission Control" where the IP Policy Control is effectively a Policy Decision Point (PDP). The IP Policy Control makes decisions in regard to network based IP local policy using policy rules, and communicates these decisions to the IP BS Manager in the GGSN, which is the IP Policy Enforcement Point (PEP).

A protocol interface between the IP Policy Control and local application servers/proxies (e.g. local SIP proxy) support the transfer of policy related information from the application layer to the policy decision point. *(Editorial note: The exact mechanisms, protocols whether proprietary or standardized, and how they are used are for further study.)*

A protocol interface between the IP Policy Control and GGSN support the transfer of information and local policy decisions between the policy decision point and the IP BS Manager in the GGSN. *(Editorial note: The exact mechanisms, protocols whether proprietary or standardized, and how they are used are for further study. One possible candidate is the COPS protocol [RFC2748] which describes a simple query and response protocol that can be used to exchange policy information between a policy server (PDP) and its client (PEP). Where RSVP is used as the signalling protocol in the IP bearer level, a COPS protocol variant carrying embedded RSVP information, i.e., COPS-RSVP, defined in [RFC2749] may be used.)*

(Editorial note: Additionally, the IP Policy Control may have protocol interfaces to other devices (e.g., AAA, bandwidth broker) which support transfer of information (e.g., authentication, availability of resources, etc.) for use in local policy decisions. These are for further study.)

(Editorial note: Where the access point of the APN is not located at the GGSN, the location of policy enforcement point is for further investigation. The IP policy architecture for cases where the access point

of the APN is located in a third party network, e.g., a corporate network, is for further study.)

Resource Manager

Within the UMTS network, there is resource management performed by various nodes in the admission control decision. The resources considered here are under the direct control of the UMTS network.

In IP Networks, it is also necessary to perform resource management to ensure that resources required for a service are available. Where the resources for the IP Bearer Service to be managed are not owned by the UMTS network, the resource management of those resources would be performed through an external resource management function for the IP network.

In addition, where the UMTS network is also using external IP network resources as part of the UMTS bearer service (for example for the backbone bearer service), it may also be necessary to interwork with an external IP resource manager.

Figure 9-1 shows the scenario for control of an IP service using IP BS Managers in both possible locations in the UE and Gateway node and an external Resource Manager. The figure also indicates the optional communication path between the IP BS Managers in the UE and the Gateway node.

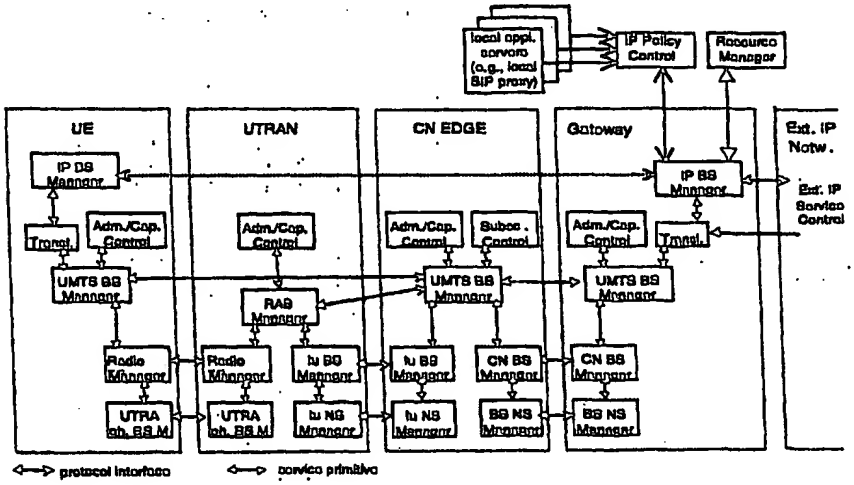


Figure 9-1: QoS management functions for UMTS bearer service in the control plane for an external IP Service

Note: This does not cover the cases of a circuit switched service, or an IP service interworking with an ATM service at the gateway node.

Editorial note: The actual split of the UE into separate elements (as described in TS 23.002 and TS 24.002) as well as the terminology regarding the UE elements and the distribution of functionalities between the UE elements is for further study. The modeling of the UE in TS 23.107 is not in line with TS 23.002 and TS 24.002, which makes this clarification necessary.

~~Editorial note: The addition of policy functionality to the QoS framework described here is for further study. The location of the policy related functionalities is for further study as well.~~

Editorial note: Elements external to the nodes are used to highlight and explain possible solutions to requirements that have been identified within the QoS drafting group. If elements or interfaces are specified or mandated within 3GPP, they shall be included in the Reference Architecture.

Title: Application of IP Policy Architecture in UMTS

1 INTRODUCTION

This contribution considers the requirements as outlined in contribution S2-000723 and subsequent discussion, and examines how those requirements could be met by application of policy control using the architecture proposed in contribution S2-000840.

2 DESCRIPTION

2.1 Requirements

The requirements derived from contribution S2-000723 and subsequent discussions are identified below. Note that the derived requirements as stated here have no status and are not recognised as formal requirements within 3G.PP. Furthermore, the requirements listed below are not assumed to be a definitive or complete set of requirements for the problem space identified in that contribution.

Additional discussion is recommended to increase the understanding of the specific requirements, which could enable an even broader range of solutions. In some cases, the requirements stated have been logically extended to cover additional functions, and/or possible alternate options have been proposed. Hence, this contribution is aimed to invite further discussion of both the proposed solution and the requirements. In the discussion below, the requirements are described in relation to a telephony call being placed over an IP based telephony network. However, the requirements for the controls are equally applicable for multimedia service, and for other types of applications entirely.

1. Restriction on establishment of UMTS bearers
   The requirement stated was that the conversational bearer may only be permitted for use with the AT&T telephony network. This requirement could logically be extended to have control over different types of bearer, dependant on the either the network they are connecting to (i.e. the APN), or the application that they are they are working towards. Although the former function may be useful, it is assumed that the latter case is the requirement. The requirement is logically extended to allow restriction of the bearer types to be controlled from any application.

Theft of Service:
There were several requirements that were raised under the banner of "theft of service". These are discussed individually.

2. Access to resources within the telephony network is restricted by gating applied from the application level (i.e. an application server such as a SIP proxy can restrict access to the service network resources). The gating shall enforce that communication across the telephony network is only according to the connections approved from the application server.

3. The telephony service based charging for data transfer (active phase of call) is not started until some time after the access bearer resources are reserved. The user cannot use these bearer resources without charge. The original stated requirement was that the user was not permitted to utilise access network resources prior to the start of charging. A proposed alternatives is:
   - The user shall be permitted to utilise access network (e.g. UMTS) resources prior to the start of call charging, but that a charging rate specific for the access bearer would be applied for unauthorised data flow prior to the active phase.
   - Alternatively, the access bearer may be closed down if it is used fraudulently and no access network charging is applied.

- In addition, resources that are not authorised and charged appropriately should not be permitted to be reserved.

Note that the solution overview below describes the flow of information between nodes to allow the policy decisions to be made in this way for this application. However, this contribution does not propose that the application is designed in this way, or that IP policy control should be used in the manner indicated. Rather, this contribution is simply giving an example of how policy control may be utilised within this architecture.

However, alternative solutions may be used where various policy decisions are not outsourced to the IP Policy Control, but are made locally within the node. This contribution does not propose whether or not these decisions should be outsourced; it merely shows what is involved if they are outsourced.

2.2 Solution Overview

An overview of how the requirements can be met using "policy" mechanisms is discussed. Further detailed analysis can be performed when the requirements are clarified. The architecture for IP policy control specified in contribution S2-000840 is applied. This architecture is shown in the figure below.

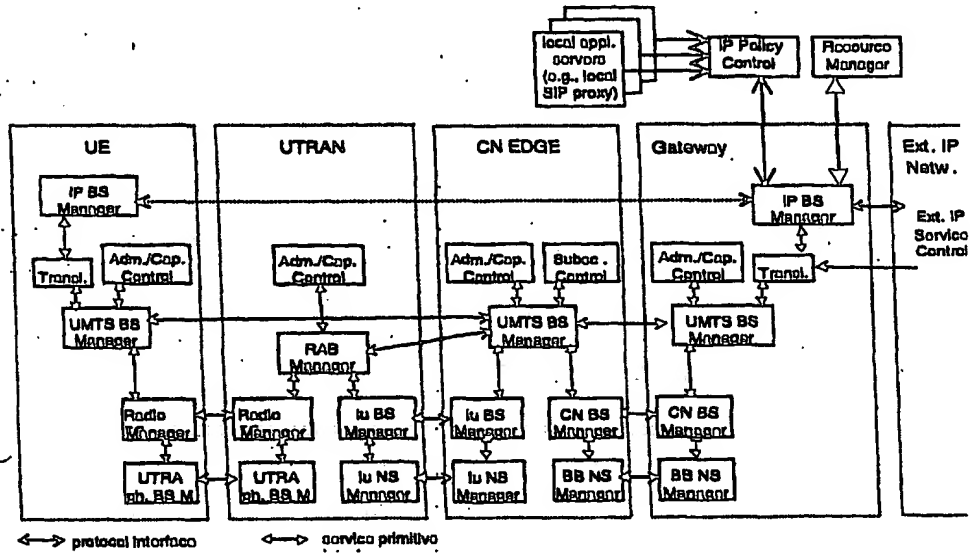


Figure 1 Basic Architecture

An information flow is described below, which is depicted in figure 2.

The end hosts initiate the application, in this case a telephony call, using SIP signalling (1). The SIP signalling passes through a SIP proxy server within the network. The SIP session identifies the end points within the telephony network, denoted by their IP addresses. These IP addresses both reside within the addressing space of the telephony network (if the call does not terminate within this telephony network, the addresses are the gateway address within the telephony network which the bearer passes through).

After the session has been started, the UE will need to establish the QoS enabled access bearer for the data plane. This may occur during the session establishment as part of the pre-conditions for the session. The UE must select the access bearer type to be used based on the required characteristics, such as a conversational bearer, and it initiates a PDP context for the bearer level.

The UE then requests establishment of the UMTS bearer (3). The translation/mapping function in the GGSN maps the UMTS bearer service into a detailed description of an IP service that is being provided to be user over the access network. The IP BS Manager contacts the IP Policy Control to determine whether this access IP bearer service is permitted to be established (4). The IP Policy Control may apply rules that restrict the use of specific access bearers dependent on network factors such as involvement of the Local SIP Proxy Server. Since the IP Policy Control has been informed that the Local SIP Proxy Server is in use for this connection, the use of this bearer type is approved.

Authority to establish the access bearer is separate from authority to transmit data into the telephony network. When the bearer is established, a "gate" is established at the GGSN that controls what data is permitted to enter the telephony network (6). This gate is similar to the DS edge functionality, performing classification and policing of the data. The gate is controlled by data received from the application through the IP Policy Control.

Prior to the session reaching the active phase, the UE may send data regarding the proposed usage of the access bearer to the GGSN. This information may be sent to the GGSN either through IP level signalling such as RSVP, or it could alternatively occur through PDP context signalling, as proposed in contribution S2-000842 for the uplink direction. For the downlink direction, the PDP context signalling already includes information about the TFT filters. In the figure below, the proposed bearer usage information is passed through PDP context signalling.

When the GGSN receives information about the traffic usage for this bearer, the IP BS Manager may authorise the usage of the bearer (5). If the proposed usage does not agree with that authorised by the SIP proxy server, the GGSN may reject the bearer establishment, or the session establishment in the case of RSVP. The SIP proxy server by this time must have supplied information to the IP Policy Control regarding the authorised traffic descriptor.

When the session reaches the appropriate state (i.e. the active phase), the gate is opened to allow the data from the user to enter the network (7).

When the session is finished, the SIP proxy server revokes authorisation for both the session and the bearer level. It shall also close the "gate" that has been opened from the GGSN towards the telephony network. This action occurs at several different levels. The SIP proxy server terminates the session directly to the UE. It sends information to the policy server which results in the closing the gate at the GGSN. Finally, the SIP proxy server sends information to the policy server that results in the termination of the bearer, if the bearer termination has not already been initiated from the UE.

The figure below shows a simple overview of the information flow between the network elements. The actual protocols and messages that would be used within this flow are for further study.

3

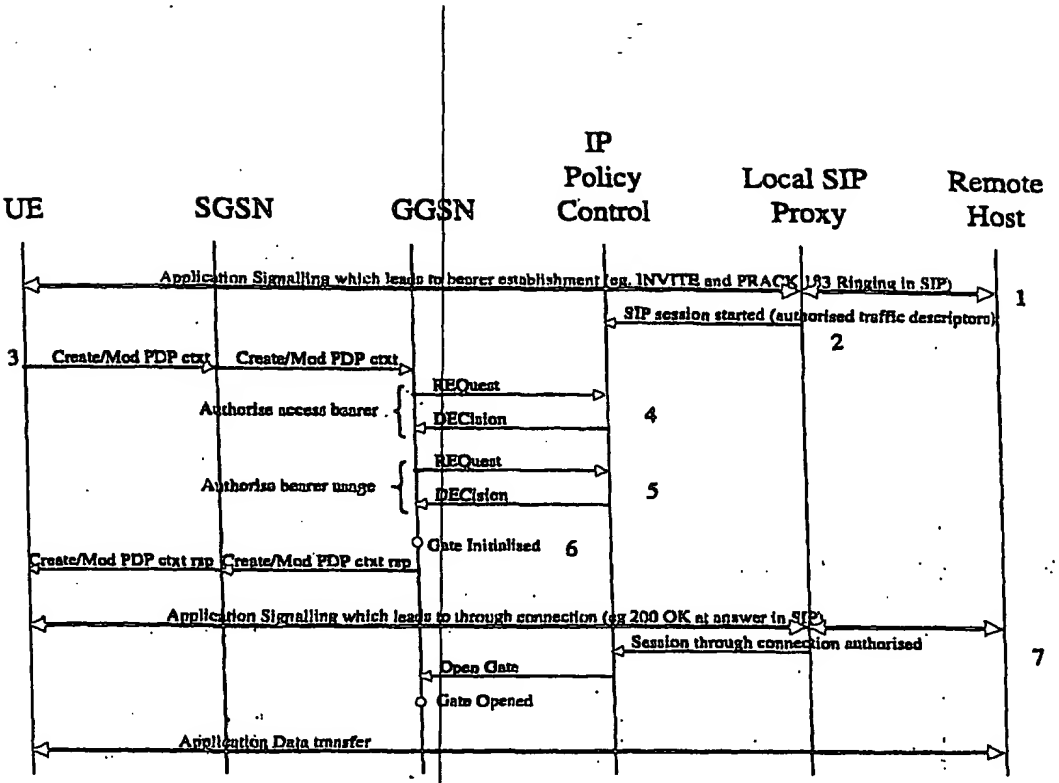


Figure 2 Information Flow

Some additional comments can be made to the proposal described above.

An aim with this proposal is that the functions required at the GGSN are not application specific, and may be required for different applications. Therefore, the interface from the GGSN to the IP Policy Control should be a standardised interface for control of these functions. It is for further study what this protocol interface should be.

The IP Policy Control may receive information from different applications that want to apply control. Although the function they are applying control to within the GGSN may be the same, the actual information supplied by the application and how that information is used may be different for different applications. Therefore, there may be a range of protocols between the IP Policy Control and the applications, although it is recommended that applications with similar policy controls use the same protocol.

Requirement 1 specifies that the use of specific access bearers will be restricted dependent on not just the application, but that the application (in this example the telephony call) determines whether the bearer type is authorised for use. To enable this control, a SIP proxy that is permitted to perform this authorisation (this must be a trusted node within the network with this responsibility) communicates to the IP Policy Control that the Local SIP Proxy Server is involved in the call for this UE.

For scenarios where the UMTS bearer is being established to other networks (i.e. where the APN is not accessed from the serving network), the normal UMTS policy mechanisms may be used to apply control over establishment of the UMTS bearer services.

Requirement 3 states that resources that are not authorised and charged appropriately should not be allowed to be reserved. The control information from the SIP proxy server designates not only that the call is using the Local SIP Proxy Server, but also that the session is in an appropriate state to authorise the bearer service. When the IP BS Manager in the GGSN contacts the IP Policy Control, the IP Policy Control makes a decision on not just whether the UE is authorised for the bearer type, but that the application has approved the connection to be made at this time.

A possible alternative to this mechanism is to allow the bearer service to be established independent of the session state. In this case though, the charge applied for the access bearer would be different dependent on the current session state. If the session exists, there may be no access bearer charge, but if it doesn't exist, there may be access bearer charges even if any data sent on the bearer is subsequently discarded.

Requirement 2 specifies strict control the destination for data that is allowed to enter the telephony network. This may be because the telephony service could have destination dependent charging, and also because it may be performing resource reservation for the connection. In order to provide this control, the "gating" function in the GGSN must receive configuration data from the SIP proxy server via the IP Policy Control.

If the UE does not provide signal proposed usage information for the connection, the network can only verify correct usage of the service network by checking the received data against the gate, and it cannot perform any additional resource management checks. Reception of traffic profile information allows the UE to verify its' intended usage is authorised, and permits additional negotiation of IP level resources.

There are different actions within the policy enforcement that may be applied by the IP BS Manager. For example, if data is received that is not allowed through the gate, the IP BS Manager may take actions from discarding the data to terminating the bearer. The scope of policy enforcement options must be determined and considered when selecting the protocol to be used between the IP BS Manager and the IP Policy Control for each policy function..

3 CONCLUSION

Within this overview, the following requirements have been considered:

1. Authorisation of UMTS bearers from the application.
2. Control of opening and closing the gate for data to enter the service network, controlled from the application server through the policy server.
3. Control of the level and destination of data permitted to pass the gate and enter the service network, controlled from the application server through the policy server.

It has been demonstrated that the IP Policy architecture proposed in S2-000841 can be used to perform policy control in a manner enabling these requirements to be fulfilled. Therefore, it is proposed that contribution S2-000841 is accepted.

Title: End-to-end QoS Related Information Carried in the PDP Context Message

1 INTRODUCTION

In order to provide end-to-end QoS, resources need to be managed both in the UMTS network and in the external IP network. This contribution examines how the PDP context can be used to provide information that is necessary to control end-to-end QoS. The solution discussed in this document is applicable e.g. in the situation where the UE does not provide an IP BS Manager. Note that this scenario was described in S2-000813.

2 DISCUSSION

2.1 End-to-end QoS Related Requirements

The end-to-end QoS negotiation requirements listed in Section 9.1 of TR 23.821 include the following two requirements:

- *The UMTS QoS negotiation mechanisms used for providing end-to-end QoS shall not make any assumptions about application layer signaling protocols.*
- *The UMTS network shall be able to negotiate end-to-end QoS also for mobile terminals and applications that are not able to use QoS negotiation mechanisms other than the ones provided by UMTS.*

End-to-end QoS provisioning implies that resources in the external IP network need to be managed by the IP BS Manager in the GGSN. There are different IP resource management techniques available for the IP BS Manager to manage the IP resources, and some of these imply call admission control (CAC) functionality in the GGSN. In order for the GGSN to exercise CAC, information about the IP traffic (e.g. average and peak rates, required QoS and destination) may be necessary.

The first requirement above implies that the initiating terminal cannot rely on application level signaling to check whether resources are available through the network and at the remote access. It follows that such a resource check must be performed at the bearer level. If the UE does not perform this bearer level request, then the GGSN may need to perform this function, and requires information about the destination IP address in order to perform a CAC decision.

The second requirement listed above implies that end-to-end QoS must be provided even for terminals that do not implement the IP BS Manager functionality and only use UMTS BS Manager (e.g. PDP context signaling) to request resources within the UMTS network.

From these requirements and the discussion above it follows that the UE may need to signal end-to-end QoS related information to the GGSN. We propose that this piece of information be added as a new information attribute to the

1

existing PDP context. This end-to-end QoS attribute shall be transparent to the UMTS network and may be piggybacked within the existing PDP context signaling.

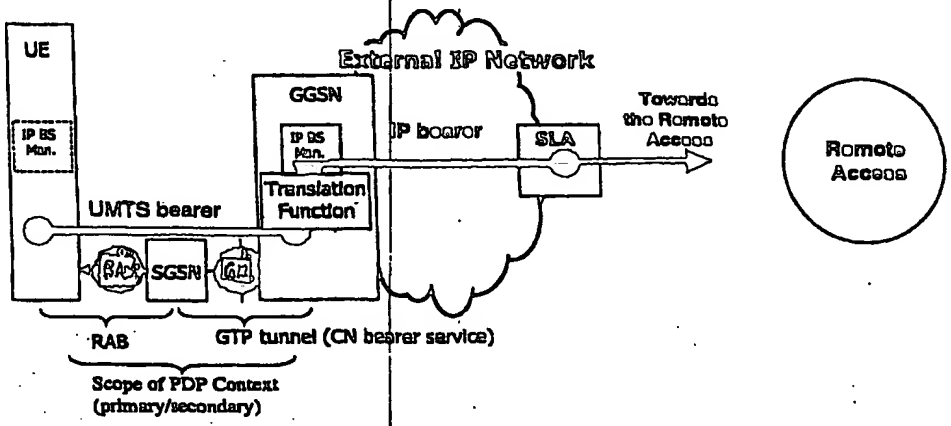


Figure 1: Schematic diagram of the assumed network model

2.2 Possible Extensions to the PDP Context

The appropriate extension of the PDP context depends on the IP BS functionality that is actually implemented in the GGSN. Depending on the scope of the CAC in the GGSN, we distinguish the following two cases:

Case 1: CAC is based on the availability of resources over which the GGSN has control

In this case the necessary QoS information may be extracted from the existing PDP context by the Translation Function between the UMTS BS Manager and the IP BS Manager. In order to facilitate efficient IP resource usage and allow for policy decisions based on RSVP parameters, the PDP context could carry additional QoS related information specific to the IP bearer. For instance, such an additional parameter can specify traffic descriptors and QoS descriptors. Such descriptors may be based on the ones associated with standard IP mechanisms, such as the differentiated services or integrated services. Alternatively, these descriptors may be based on the concept of the generic IP bearers.

Case 2: The CAC is additionally based on the resource situation at the egress SLA

In this case the destination IP address needs to be carried in the PDP context (apart from the descriptors of Case 1).

The exact form of this additional QoS attribute in the PDP context is for further study. Candidates for the basis of this attribute include:

- parameters associated with the differentiated services framework
- parameters associated with the integrated services framework
- generic IP bearer parameters

2

3 PROPOSAL

It is proposed that 3GPP S2 consider the arguments raised to extend the PDP context with an additional attribute having end-to-end QoS significance.

We propose the following text to be added to Section 9 of TR 23.821:

9.x IP Level End-to-end QoS Attributes
[Editor's note: The contents of this section is intended to be included in a new subsection 6.4.y of TR 23.107]

In order to allocate IP resources in an external network and to execute CAC the PDP context may contain the optional attribute "End-to-end QoS". The content of this optional attribute is for further study. This attribute is transparent to the UMTS BS Manager, but allows the transport of IP QoS related information.

It is also proposed that a new subsection be added to Section 6.4 of the document TR. 23.107 "QoS Concept and Architecture":

6.4.y IP Level End-to-end QoS Attributes

4 REFERENCES INCORPORATED BY REFERENCE

[1] TR 23.821 "Technical Specification Group Services and System Aspects; Architectural Principles for Release 2000"

[2] TSG-S2 S2-000813, "QoS Conceptual Models"

[3] TR 23.107 "Technical Specification Group Services and System Aspects; QoS Concept and Architecture, Release 1999"